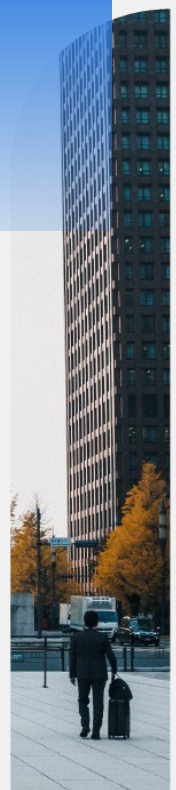
Log4Shell (Log4J)

CVE-2021-44228, 4422, 45046, 45105 & More

Outbreak Alert & Analysis

Derek Manky & Aamir Lakhani

FortiGuard Labs



Disclaimer

- Intended for internal Fortinet use
- We are not detailing the vulnerability how it works
- Information is updating please refer to the Outbreak Alert and Threat Signal page on the FortiGuard website
- PSIRT information on Fortinet product status can be found at: https://www.fortiguard.com/psirt/FG-IR-21-245

Resources

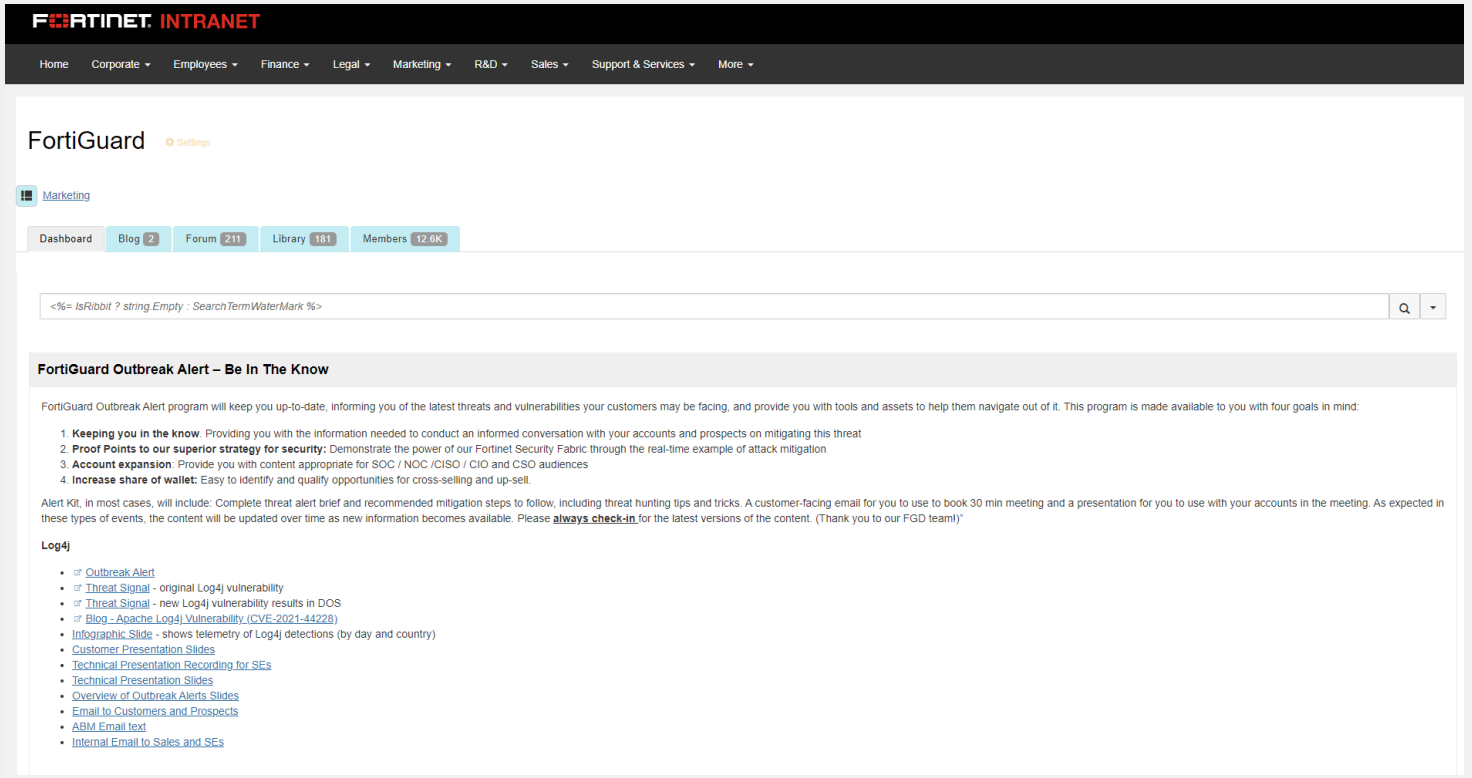
FUSE→ Marketing → FortiGuard Labs → Outbreak Alert Index

Assets on FUSE:

- Outbreak Alert
- Threat Signal - original Log4j vulnerability (2.14.1)
- Threat Signal - new Log4j vulnerability results in DOS (2.15.0)
- Threat Signal – second DOS vulnerability (2.16.0)
- Blog - Apache Log4j Vulnerability (CVE-2021-44228)
- Infographic Slide - shows telemetry of Log4j detections (by day and country)
- Customer Presentation Slides
- Technical Presentation Recording for SEs
- Technical Presentation Slides
- Overview of Outbreak Alerts Slides
- Email to Customers and Prospects
- ABM Email text
- Internal Email to Sales and Ses
- PSIRT Advisory

In Progress:

New blog on reports of ‘wormable’ Mirai variant



Fortinet.com Outbreak Alert Page

FORTINET

ENTERPRISE | SMALL MID-SIZED BUSINESSES | SERVICE PROVIDERS | PARTNERS

NETWORK SECURITY | CLOUD SECURITY | SECURITY OPERATIONS | ZERO TRUST ACCESS | NETWORKING AND COMMUNICATIONS | SECURITY-AS-A-SERVICE | DISCOVER MORE

FortiGuard Outbreak Alerts: Click here for the latest information on Log4j

FortiGuard Outbreak Alerts

Tactical steps to mitigate the latest cybersecurity attacks

2021 Gartner® Magic Quadrant™ for Network Firewalls →

Outbreak Alert

When a cybersecurity incident/attack/event occurs that has large ramifications to the cybersecurity industry and affects numerous organizations, **FortiGuard Outbreak Alerts** will be the mechanism for communicating important information to Fortinet's customers and partners. These Outbreak Alerts will help you understand what happened, the technical details of the attack and how organizations can protect themselves from the attack and others like it.

The Outbreak Alerts we have tracked and analyzed can be seen below. To see information on the latest cyber threats we are tracking, please refer to the **Threat Signals** listed in the box to the right.

Threat Signals

Apache Log4J Remote Code Execution Vulnerability (CVE-2021-44228)
FortiGuard Labs is aware of a remote code execution vulnerability in Apache Log4j. Log4j is a Java b ...

Dec 14, 2021 ID: 4335

NICKEL - Targeting Organizations Across Europe, North America, and South America
FortiGuard Labs is aware of reports relating to NICKEL, a state sponsored group targeting varying in ...

Dec 07, 2021 ID: 4330

Joint CyberSecurity Advisory on Attacks Exploiting Zoho ManageEngine ServiceDesk Plus Vulnerability (CVE-2021-44077)
FortiGuard Labs is aware of a recent joint advisory released by the U.S. Cybersecurity and Infrastru ...

Dec 06, 2021 ID: 4329

Click here to access all Threat Signals »

Dec 9, 2021

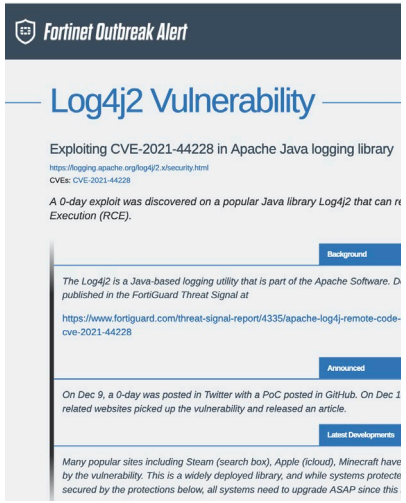
Log4j

Attack Type: Vulnerability Exploitation Leading to Remote Code Execution
Threat Actor: Multiple unidentified attackers

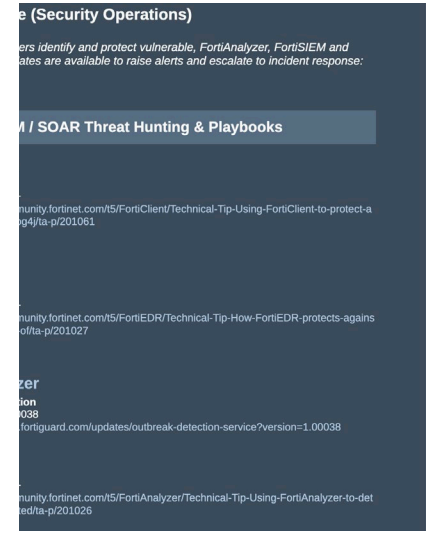
A zero-day vulnerability was discovered in Log4j, a Java-based logging utility that is part of Apache Logging Services Project. Deployed on millions of servers, this vulnerability can be exploited to allow for remote code execution and total system control on vulnerable systems.

Log4j Outbreak Alert

FortiGuard Outbreak Alerts



Threat Hunting tools from Fortinet to help you determine if you were affected



An attack overview, its
and the technology a

lunting tools from Fortinet
ou determine if you were
affected

FortiGuard Outbreak Alert Coverage

Log4j

December 9, 2021

Attack Type: *Vulnerability Exploitation Leading to Remote Code Execution*

Threat Actor: *Multiple attackers*

A zero-day vulnerability discovered in Log4j, a Java-based logging utility that is part of Apache Software that i deployed on millions of servers. By getting a specific text string to be logged, the vulnerability can be exploited to enable remote code execution and total system control on vulnerable systems.

Background

The Log4j2 is a Java-based logging utility that is part of the Apache Software. Detailed background is published in the FortiGuard Threat Signal at

https://www.fortiguard.com/threat-signal-report/4335/apache-log4j-remote-code-execution-vulnerability-cve-2021-44228

Announced

On Dec 9, a 0-day was posted in Twitter with a PoC posted in GitHub. On Dec 10, several security-related websites picked up the vulnerability and released an article.

Latest Developments

Popular sites such as Steam (search box), Apple (icloud), Minecraft have been confirmed affected by the vulnerability.

Apache Log4J Remote Code Execution Vulnerability

(CVE-2021-44228)

Nov 24
2021

Apache was notified about the **Log4j remote code execution vulnerability** by the Alibaba Cloud Security team.

Dec 9
2021

The exploit proof of concept was then posted to Github at **15:32 GMT**

on December 9, 2021, and the first attempts to trigger callbacks were seen **82 minutes later**.

Dec 10
2021

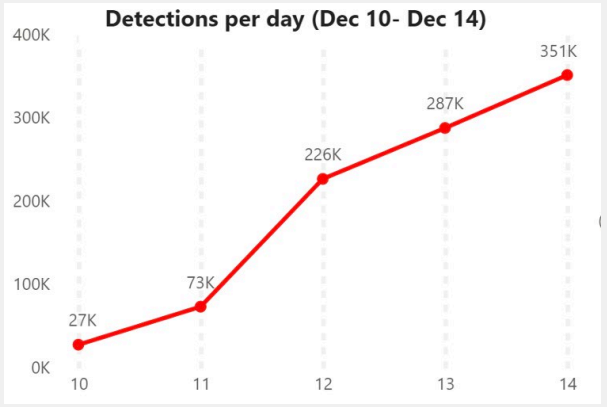
FortiGuard Labs released Threat Signal report and a blog with initial analysis and Fortinet product protections

Apache and CISA provide technical details and mitigation recommendations on the Log4j vulnerability.

Threat Signal Report:
https://www.fortiguard.com/threat-signal-report/4335/apache-log4j-remote-code-execution-vulnerability-cve-2021-44228

Threat Encyclopedia:
https://www.fortiguard.com/encyclopedia/ips/51006

Outbreak Alert:
https://www.fortiguard.com/outbreak-alert/log4j2-vulnerability



Massive scanning and exploitation activity detected. Crypto Miner and Botnet malware dropped by attackers

FortiGuard Labs detects Mirai Botnet Malware activity distribution on vulnerable systems

Adware/Mirai
ELF/Mirai.A!tr
ELF/Mirai.B!tr
ELF/Mirai.IA!tr
Linux/Mirai.B!tr.bdr
Linux/Mirai.BMQ!tr
Linux/Mirai.SEMR!tr

FortiGuard Labs detects Cryto Miner Malware activity distribution on vulnerable systems

Adware/Miner
BASH/CoinMiner.RZ!tr
BASH/Miner.BO!tr.dldr
BASH/Miner.OO!tr
ELF/BitCoinMiner.HF!tr
ELF/CoinMiner.CFA!tr
Riskware/CoinMiner.PO
Riskware/Miner
W64/CoinMiner.PO!tr
W64/HarHarMiner.A!tr

FortiGuard Labs

Apache Log4J Remote Code Execution Vulnerability (CVE-2021-44228)

Apache Log4j2 2.14.1 and below are susceptible to a remote code execution vulnerability where a remote attacker can leverage this vulnerability to take full control of a vulnerable machine.

Total Detections

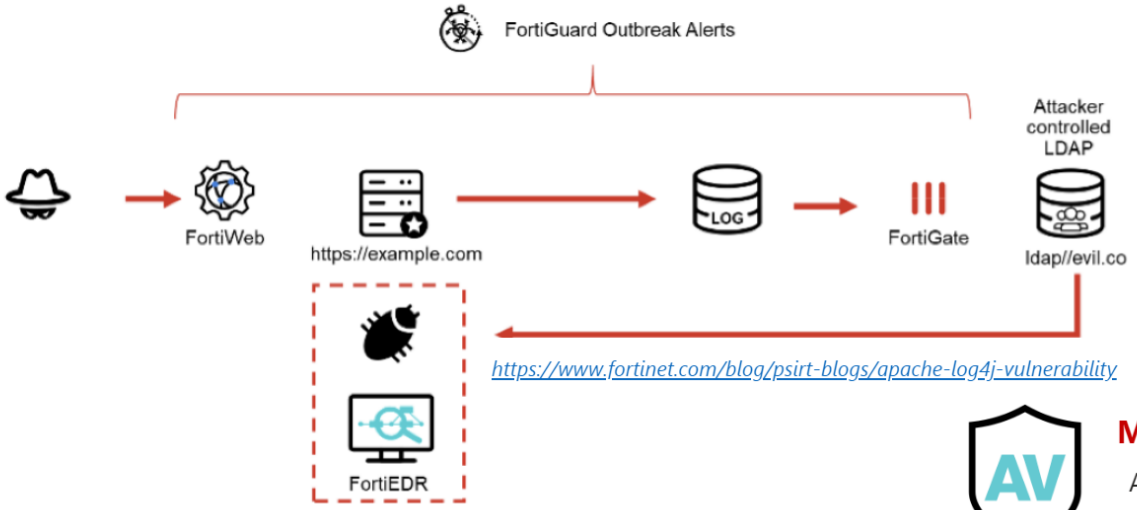
+160M

IPS

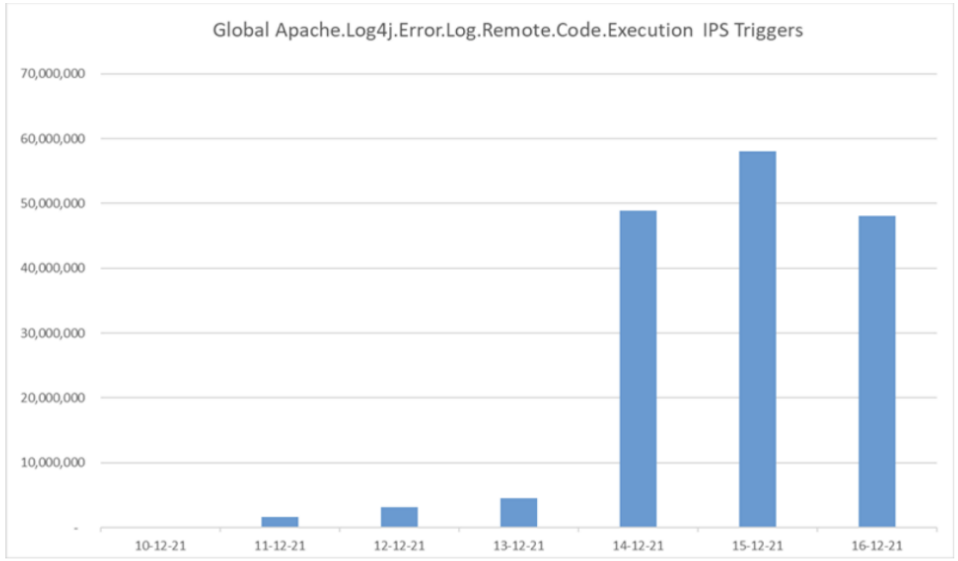
ID	51006
Created	Dec 10, 2021
Updated	Dec 13, 2021
Outbreak Alert	Log4j2 Vulnerability
Severity	●●●●●
Coverage	IPS (Regular DB) IPS (Extended DB)
Default Action	drop
Active	✓
Affected OS	All
Affected App	Apache

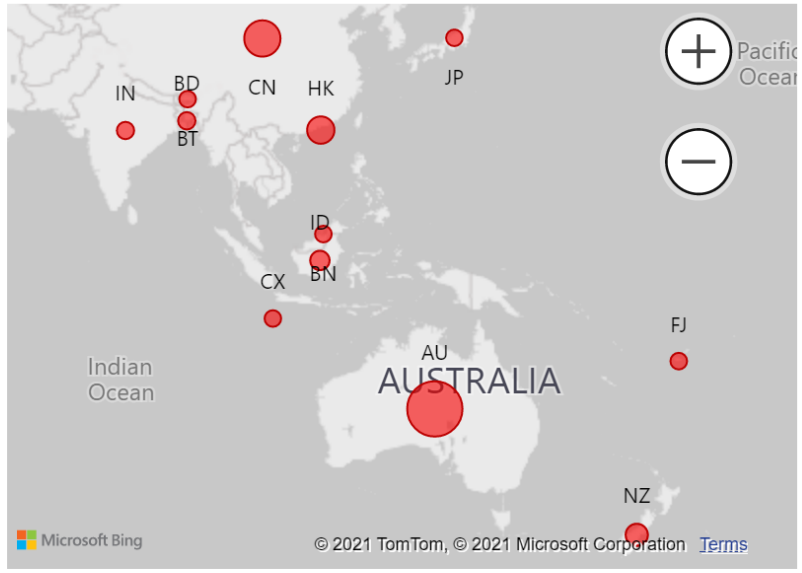
Fortinet Security Fabric

FortiGuard Labs has created an Outbreak Alert for this incident which allows customers to track indicators of compromise (IOCs) and apply protections against this issue using the Fortinet Security Fabric.



https://www.fortinet.com/blog/psirt-blogs/apache-log4j-vulnerability





AV

MIRAI

AV Signatures
Adware/Mirai
ELF/Mirai.A!tr
ELF/Mirai.B!tr
ELF/Mirai.IA!tr
Linux/Mirai.B!tr.bdr

Crypto Miner

AV Signatures
Adware/Miner
BASH/CoinMiner.RZ!tr
BASH/Miner.BO!tr.dldr
BASH/Miner.OO!tr
ELF/BitCoinMiner.HF!tr

Aditional Resources

Threat Signal Report:
https://www.fortiguard.com/threat-signal-report/4335/apache-log4j-remote-code-execution-vulnerability-cve-2021-44228

Outbreak Alert:
https://www.fortiguard.com/outbreak-alert/log4j2-vulnerability

PSIRT Advisories:
https://www.fortiguard.com/psirt/FG-IR-21-245

Threat Encyclopedia:
https://www.fortiguard.com/encyclopedia/ips/51006

Vulnerability

- Log4J is the software. The vulnerability is being called Log4Shell
- Version 2 thru version 2.16.0 (with intermediate fixed found in 2.15.0 and 2.16.0)
- Clients that cannot upgrade can remove JndiLookup class from code:
  - zip –q –d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
- Multiple scanning tools available
  - Remember to scan multiple applications on a compute instance or container.
  - NMAP – nse-log4shell plugin
  - Full Hunt's log4j-scan
  - Syft
  - Grype

Severity

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 10.0 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

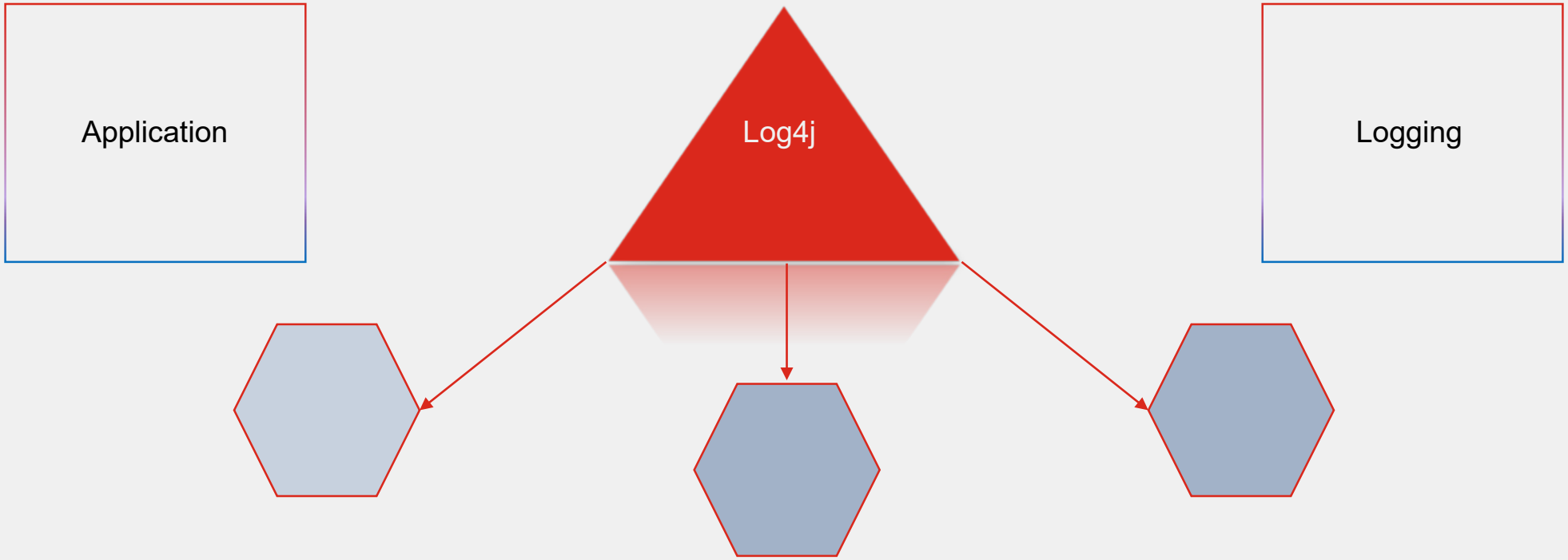
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

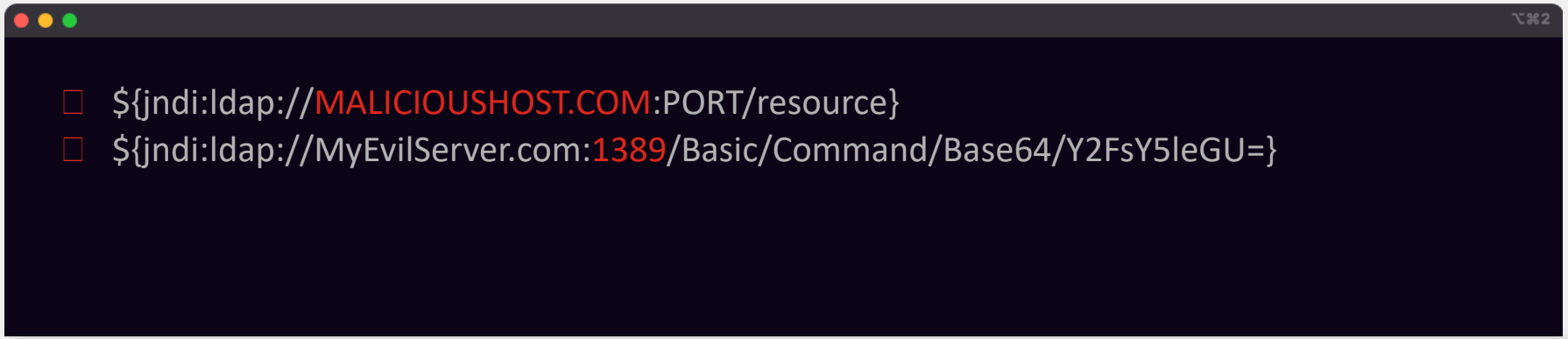
Usage Attack

- Does the attack allow for the possibility of data breaches?
- Yes, attackers have the capability of using multiple exploits using this vulnerability.
- What are common attacks being exploited by this vulnerability?
  - Ransomware, Cobalt Strike Beacons, RATs, data leakage
- Is that attack wormable?
  - It has all the characteristics of becoming wormable.
- Do client-side exploits occur?
  - Client-side exploits and mobile attacks are a possibility thru this attack
  - Many of the mobile attacks shown on carious blogs are using the mobile device as an attacker

Background

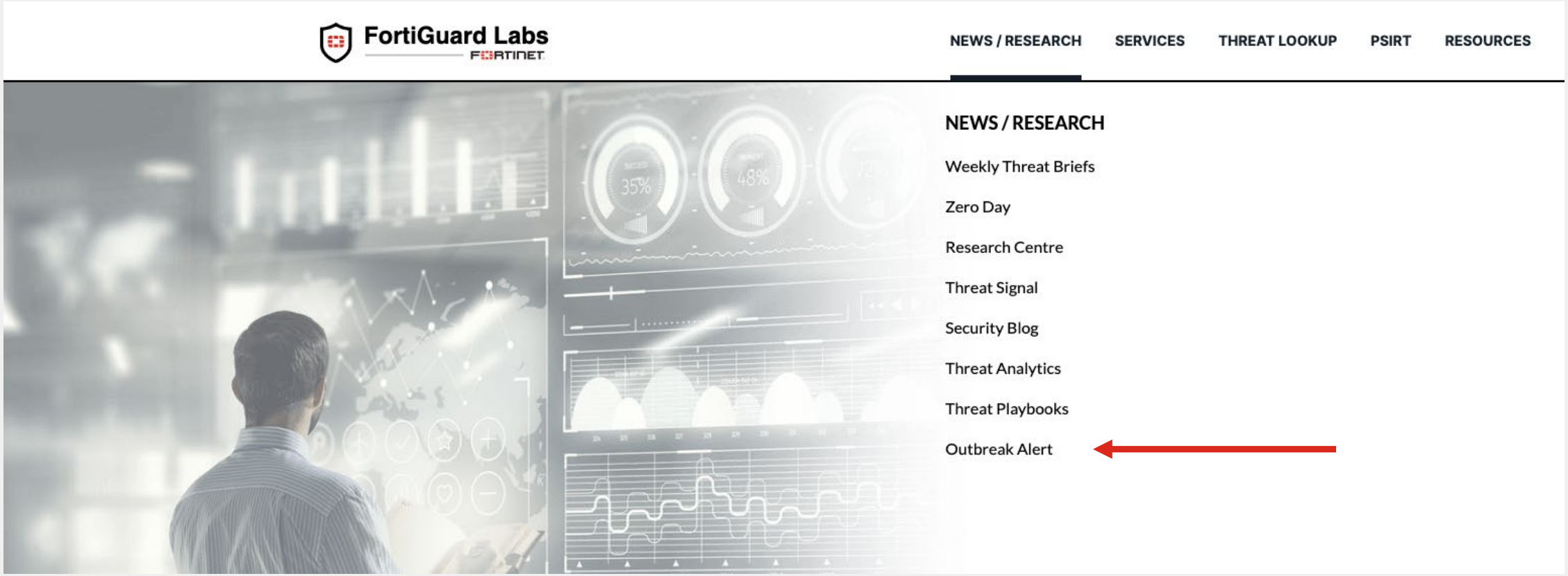


Attack Execution



- Attack has probably been present since 2013
- Proof of Concept codes are making this easy to exploit
- APT groups are chatting on how the holiday season is a perfect time to take advantage of this attack
- Library is on enterprise software, IoT devices, OT devices, cloud environments
- Log4j 2.16.0 released Dec 13th, 2021 at 19:50 EST

Outbreak Alert



Mitigation

To break the **attack sequence** and protect the organization, we need to detect and **rapidly adjust the security posture** to effectively protect against newly discovered attack's tactics **across ever expanding attack surface**.

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control
		FortiCWP	FortiGate – IPS 19.215 FortiWeb – 0.00306 FortiADC – IPS 19.215 FortiProxy – 19.215	FortiEDR	

Product Summary

FortiGate NGFW

IPS 19.220

FortiClient

19.220
6.2+

FortiAI

FortiMail

FortiCASB

FortiDeceptor

FortiCWP

21.3.0

FortiSandbox

FortiWeb

0.00307

FortiEDR

5.0

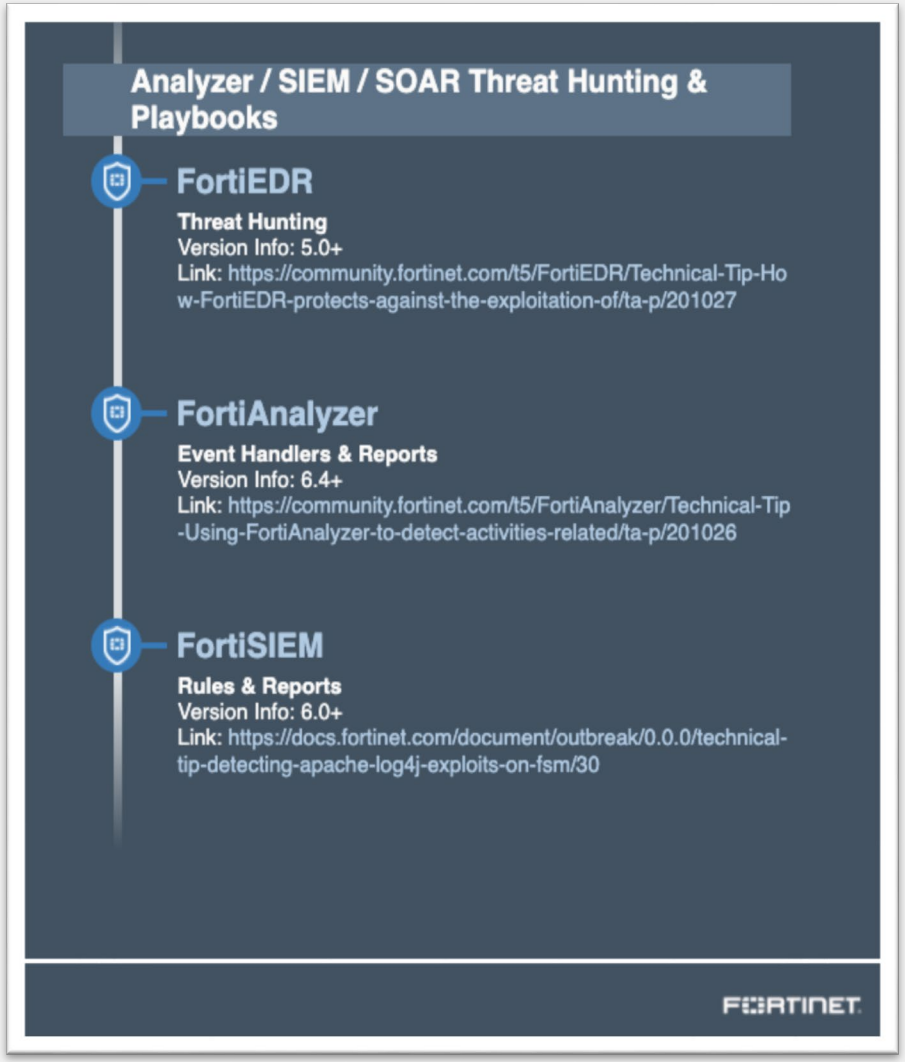
FortiAnalyzer

Event Handler
Threat Hunting Report
1.00039

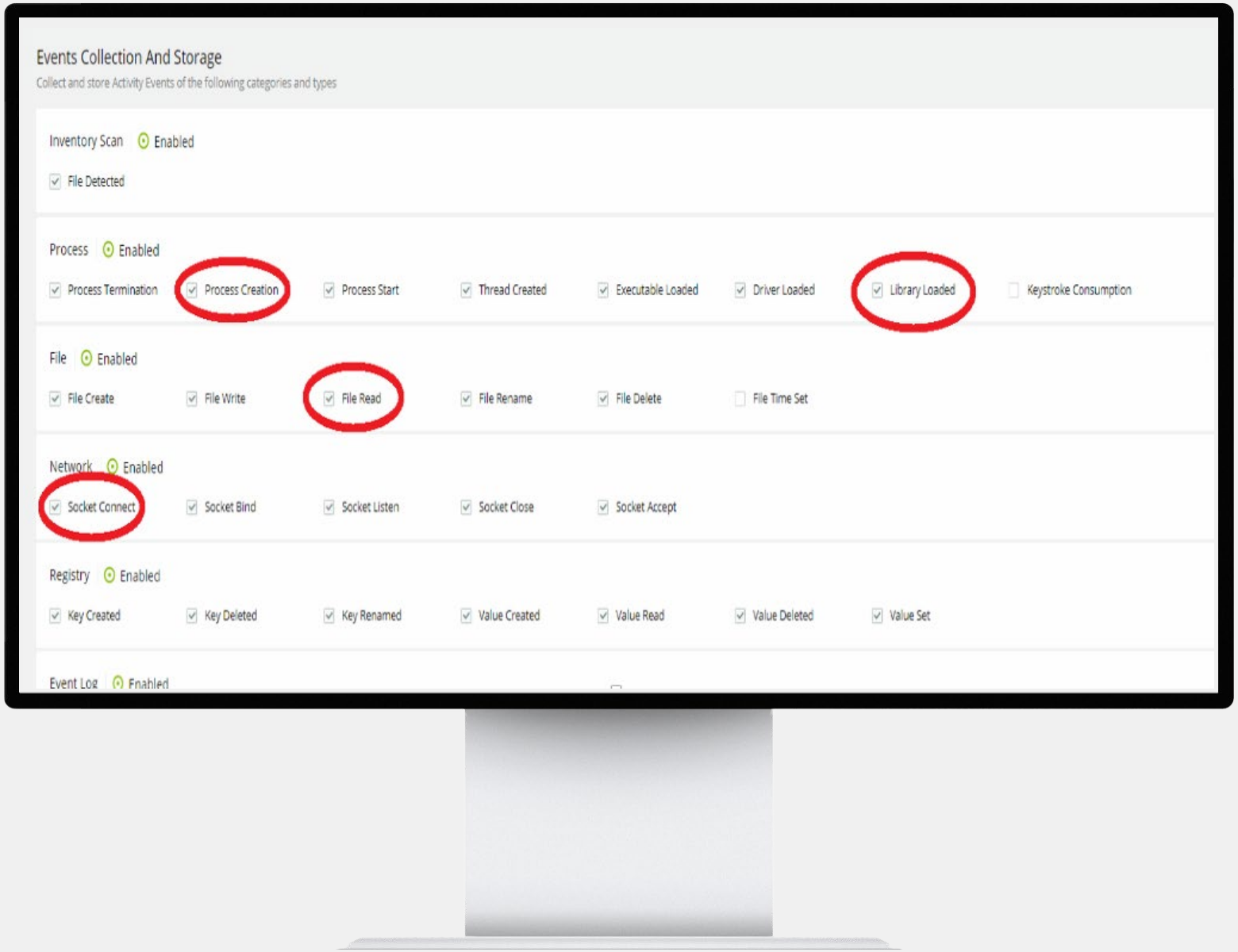
FortiSiEM

Rules &
Threat Hunting Report
6.x

FortiGuard.com



Threat Hunting



Honeypot Detection

- FortiGuard Labs is monitoring the attack thru custom built honeypots and collection nodes.

- Internal network segments can have honeypots listening on ports 80, 443, 8080. FortiDeceptor multiple decoys.
  - We do not suggest using vulnerable apps for internal honeypots because of how fast new attack techniques are being discovered.

- Honeypots should be configured for immediate alerts

Final Thoughts

- Information presented here is very preliminary information. Continue to check the outbreak alert service and the threat signal for updated information.
- Continue to check the Fortinet PSIRT advisory on the status of Fortinet products
- Attackers will leverage this vulnerability to find other vulnerabilities. We may see the exploit being taken advantage of in unexpected ways for a very long time.
- Defense in depth and security fabric solutions are going to be critical in mitigating risk.
- As of Dec 20th security researchers at Blumira have discovered a new RCE flaw via a Javascript websocket
- Free lab - https://tryhackme.com/room/solar

Questions & Answer

Aamir Lakhani
@aamirlakhani

Derek Manky
@dmanky


FORTINET